Open Access License Notice

This article is © its author(s) and is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). This license applies regardless of any copyright or pricing statements appearing later in this PDF. Those statements reflect formatting from the print edition and do not represent the current open access licensing policy.

License details: https://creativecommons.org/licenses/by/4.0/

Transforming Cyber Education thru Open to All Accessible Pathways

Sin Ming Loo
Cyber Operations and Resilience Program
College of Engineering, Boise State University
Boise, Idaho, USA
smloo@boisestate.edu
0000-0002-7395-0715

Elizabeth Khan
Cyber Operations and Resilience Program
College of Engineering, Boise State University
Boise, Idaho, USA
elizabethkhan@boisestate.edu
0009-0004-6206-5966

Eleanor Taylor
Workforce Development Program Office
NHS Directorate Idaho National Laboratory
Idaho Falls, Idaho, USA
Eleanor.Taylor@inl.gov
0009-0005-0869-9762

Char Sample
Cyber Operations and Resilience Program
College of Engineering, Boise State University
Boise, Idaho, USA
charmainesample@boisestate.edu
0000-0002-7110-470X

***Abstract*—Boise State University's (BSU) Cyber Operations and Resilience CORe program was intentionally designed so that any student, especially non-traditional and non-technical students, with an interest in cybersecurity could have an education and training pathway to enter the cyber workforce. The CORe curriculum focuses on teaching students how to design, apply, and improve cybersecurity through the interaction of people, processes, and technology. CORe is a stackable curriculum with elective credit hours and options for various academic and industry certificates and certifications that enable students to customize their unique career pathway. The CORe program guides students to think about the system being managed, the risks presented, and the dynamic intersection of system elements when considering how to incorporate resilience frameworks in achieving a resilient system. By developing systems thinking, the students gain an understanding of the interdependencies interacting with the operational system. The CORe program encourages students to integrate cybersecurity knowledge with models and frameworks found in other academic disciplines through a unifying systems approach. CORe is designed around the realities of today's broad cyber landscape: that breaches will occur in any system over time and proactive design of resilience into systems to detect, respond, and recover in a timely and orderly manner is critical. Students are taught to think holistically about cybersecurity focusing on all system elements. CORe is not a traditional cybersecurity degree. CORe is distinguished by the non-traditional engineering, computer science approach to cybersecurity education with the singular focus on infusing resilience operations and transdisciplinary systems thinking principles throughout the curriculum.**

Keywords—Non-traditional cybersecurity curriculum, Remote and asynchronous cybersecurity education model, Resilience operations, Systems thinking, Cybersecurity for Non-Cyber Students

I. INTRODUCTION

The Boise State University (BSU) Cyber Operations and Resilience (CORe) program is a comprehensive curriculum spanning multiple standalone and stackable certificates all the way to undergraduate and graduate degrees. Designed to address the emergent demand for cybersecurity professionals across disciplines, the CORe program offers flexible online and asynchronous accessible education, empowering students from diverse backgrounds to acquire vital cybersecurity skills. This is a program born from innovation, collaboration, and the unwavering commitment of stakeholders to train the next generation of cyber defenders.

The CORe curriculum focuses on learning how to design, apply, and improve cybersecurity and resilience through the understanding of elements, functions, and interaction (Meadows 2009). Elements consist of people, data, and technology. Functions are processes, and interactions define the relationships between elements and functions.

CORe is a stackable curriculum with elective credit hours permitting traditional and non-traditional students to customize their unique cybersecurity education pathway and bridge to the workforce. As part of the curriculum, students have the opportunity to earn multiple academic certificates and in-demand industry certifications. The CORe program teaches students to think about the system being managed, the risks presented, and to determine how system resilience can best be achieved with the elements of people, processes, and technology. A foundation of the CORe program is to inculcate the skill of systems thinking so students can understand the interdependencies interacting with the system in order for it to operate and, by so doing, will develop solutions inclusive of all system elements (Loo et al).

CORe is designed around the realities of today's broad cyber threat landscape: the assumption of breaches occurring in any system over time and *preemptively* building resilience into systems to detect, respond, and recover in a timely and orderly fashion is a critical requirement that constitutes the underpinning of designing secure systems. Students learn to think holistically, with the big picture, and the entire system, in mind. CORe is not a traditional cybersecurity degree, although engineering or computer science courses can be added into the CORe degree as electives. Instead, CORe is distinguished by its non-engineering and non-computer science approach to cybersecurity education and its focus on infusing *resilience* operations and transdisciplinary systems thinking principles throughout the curriculum.

The CORe foundational course, Systems Thinking, introduces students to resilience as defined by robustness,

resourcefulness, redundancy, and rapidity (Bishop 2011). This definition focuses the students to think beyond traditional robustness techniques that are part of every cybersecurity curriculum, and to consider recovery techniques included in resourcefulness and rapidity along with availability through redundancy planning. These additional discussion points provide students with an opportunity to apply models and frameworks from other academic disciplines to cybersecurity, thereby enriching the experience for both students and instructors.

II. HOW CORE PROGRAM BECAME A REALITY

The CORe program is the result of a multiyear journey of discovery and learning from cybersecurity professionals regarding the cybersecurity workforce needs. This journey began during the 2017/2018 school year when BSU started designing cyber-physical systems security courses tailored to engineering students. BSU experienced some early success with this initiative making it possible for engineering students to learn some aspects of cybersecurity before completing their undergraduate degree. These initial course offerings were rather technical and particularly popular amongst electrical engineering students.

Soon after the cybersecurity-engineering partnership successes, other students across the campus started inquiring about available security training options for non-STEM (Science Technology, Engineering, and Math) majors. During this time the signals became louder, evidencing an increased demand for a cross disciplinary approach that would permit non engineering students to understand the importance of cybersecurity. This led to the design of a non-technical certificate that allowed anyone to learn regardless of prior technical experience or aptitude. As word spread, enrollment increased, and soon the courses became self-supporting.

All the experiences and interactions with cybersecurity industry professionals culminated in the collective conviction that there was a cyber workforce challenge (Cyberseek Heatmap 2023). America's Cybersecurity Workforce Executive order (EO 13870) of May 2019 charged the Federal Government to cultivate a robust and diverse cyber workforce (EO13870 2019). Prior to that an earlier directive, Executive Order 13800 (May 2017), intended to strengthen national critical infrastructure (EO13800 2017) and upskill existing workers to keep pace with evolving technology was codified (Fed 2018, Fed 2017). Recognition of this workforce gap and the pressing need to address it presented a burgeoning window of opportunity to design a brand-new cyber certificate. This revelation prompted us to submit a grant proposal to Idaho Workforce Development Council (WDC) to develop what is now the Cyber Operations certificate. The approved funding in 2019/2020 allowed BSU to launch the 12-credit hour certificate, where students learn about offensive security, defensive security, forensics, and cybersecurity fundamentals in preparation for entry-level networking and cybersecurity industry certifications. The certificate was designed to be standalone so prospective students could enroll solely for this certificate without being in a degree program and without having any prior knowledge of cybersecurity or any technical background whatsoever.

This certificate program design was revolutionary for several reasons. First, the recruitment of working cybersecurity professionals to develop the content and bring cutting-edge cybersecurity perspectives to the coursework. Second, the whole program would be delivered online and asynchronously. The cybersecurity professionals worked with the BSU E-campus to design the courses, teach the courses, and host virtual office hours.

As this certificate became available to students in the 2019/2020 school year, a new degree concept paper was being drafted. This concept paper eventually led to the development and subsequent launch of what is now the undergraduate CORe (uCORE) and the graduate CORe (gCORE) degrees. After that WDC was petitioned to expand the initial project scope to include the implementation of uCORe and gCORe degree programs

The uCORe undergraduate degree uses the Cyber Operations 12-credit certificate as the foundation stone, adding required courses such as system thinking, risk management, various electives, and a culminating capstone. A crucial part of the uCORe program design was facilitating a practical transfer pathway for students with an associate of applied science (AAS) degree or those with technical credit hours desiring to complete an undergraduate degree. The idea being if there were not enough cybersecurity professionals in the existing cybersecurity workforce, one possible solution could be to increase the talent pool by upskilling those already possessing foundational networking and information technology training and experience. This design of this new uCORe degree was to enable those AAS students to complete an undergraduate cybersecurity degree with maximum efficiency.

Similarly, the gCORe degree was designed so that prospective students with *any* undergraduate degree could use this educational opportunity to pivot into cybersecurity. For any student interested and passionate about cybersecurity, a pathway now exists to bridge directly to the workforce.

Approval was garnered from the state board of education (SBOE) in Spring 2021 for the creation of the degrees. Now the courses needed to be built for the anticipated semester launch date of Fall 2021. Because it is an asynchronous and fully online program, the students are everywhere, and so are the instructors. Being entirely online provided the additional benefit of unlimited flexibility recruiting subject matter experts, no matter their location. The E-campus instructional designers assisted the subject matter experts to put together the individual courses and align program sequencing.

An additional challenge arose as marketing and recruiting needed to start immediately once the SBOE proposals were submitted and as courses were being built. A robust marketing and recruiting program is a necessary arm of an asynchronous online program. The CORe program relied heavily on its network of community colleges for the uCORe

degree program. The gCORe program launched with many students from College of Western Idaho and Idaho National Laboratory, along with a significant number of students that joined via the marketing outreach efforts.

This all transpired from Spring 2020 to Summer 2021 making for a very industrious and productive 18 months. The program officially launched Fall of 2021. The original business plan projects 30 to 50 students in Fall 2021. However, the program launched with 80+ students. These enrollment metrics that far exceeded initial projections are not just encouraging but also timely.

On July 31, 2023, the Whitehouse announced the National Cyber Workforce and Education Strategy (NCWES). Crafted to address the national security imperative to fill the thousands of cyber job vacancies, the strategy rests upon four pillars one of which is to 'transform cyber education.' It is noteworthy that the CORe program not only aligns with the objectives of the NCWES strategy, but that CORe, which was designed in advance of the Strategy, experienced early success with developing and strengthening regional cyber ecosystems as part of its education to workforce strategy (Whitehouse 2023). This further underscores the forward-thinking design of the CORe program and its transformational approach to delivering non-traditional cybersecurity education that is diverse and inclusive and rapidly bridges to the workforce demands.

III. THE PROGRAM AND STATUS OF ENROLLMENT

The degree plans are shown in Tables I and II. The Cyber Operations and Resilience (uCORe) degree was designed with an Associate of Applied Science (AAS) degree in mind. Two separate, but same degree plans, degrees with one for AAS transfer (Bachelor of Applied Science) and another for traditional students (Bachelor of Science) were created. This was necessary to streamline the AAS technical hours transfer process to meet the SBOE's policy.

TABLE I. BS/BAS CYBER OPERATIONS AND RESILIENCE (120 CREDITS TO UNDERGRADUATE DEGREE)

Category	**Courses**
Electives or Technical Credit Hours *(40 to 47 credits)*	From technical education courses or elective courses in student's interest
Required Courses *(30 credits)*	Cyber Systems Thinking, Cyber Project Management and Design, Cyber Capstone, Cyber Risk Management, Information Assurance and Critical Thinking, Defense Security, Offensive Security, Recovery and Forensics, Network+, and Security+
Cyber Depth *(4 to 7 credits)*	Upper division CORe courses (Risk Assessment, Cybersecurity Risk Quantification, ICS Cybersecurity, Applied Cybersecurity Programming, Machine Learning, Security Operations Center, Cyber Business and Regulatory Operations, Cyber Red and Blue Teams, Cyber Threat Intelligence, Cyber Resilience Systems Design
Applied Learning *(2 to 6 credits)*	Experience Learning, Prior Learning, Certification, and Internship
General Education *(37 credits)*	University foundations requirements

TABLE II. MS CYBER OPERATIONS AND RESILIENCE (30 CREDITS TO GRADUATE DEGREE)

Category	**Courses**
Required Courses (*4 credits*)	Cyber Systems Thinking, Cyber Risk Assessment
Foundations (*24 credits*)	Zero Trust Architecture, Cybersecurity Risk Quantification, Information Assurance, Applied Cybersecurity Programming, Artificial Intelligence and Machine Learning, Introduction to Deep Learning, Internet of Things Architecture, Cyber-Informed Engineering, Cyber Security Operations Center, Red and Blue Teams, Cyber Business and Regulatory Operations, Cyber Risk Management, Cyberlaw Ethics Policy, Cybersecurity Governance Compliance, Cyber Resilience Systems Design, Network Design and Exploitations Techniques, Resilience Coding and Architecture of Devices, Cyber Threat Intelligence, Cyber Warfare and Conflicts, Cyber Digital and Signal Intelligence
Culminating Activities (*2 credits*)	Teaching, Project with publication, or certification

For those students without AAS or technical credits, they will have many elective credit options to choose from to strengthen their learning and knowledge foundation. As cybersecurity is about people, processes, and technology, students have the opportunity to enroll in anthropology, psychology, management, supply chains, programming, or engineering courses. The objective was to provide cross disciplinary course options to expand their horizons along with their ability to synergize and integrate knowledge from different disciplines.

The required credit hours are 30 which consists of courses in thinking, risk assessment, and project management, as well as preparing students for Network+ and Security+ certificates. The Network+ and Security+ preparation is included with the mindfulness that these certifications are not the be-all and end-all, and while the courses introduce systems things and resilience concepts, they are not necessarily the fully definitive source on systems or resilience thinking. This is why the curriculum has been designed with systems thinking as one of the required courses. Our research showed cybersecurity professionals really need to understand the environment and the larger context to apply cybersecurity principles and solutions correctly and appropriately in order to provide solutions that extend beyond the typical "patch and fix" solution. Various cybersecurity frameworks and knowledge units are used to build the curriculum. However, even so, those frameworks are not the cornerstone of the CORe program. CORe is emphatically disinclined to graduate homogenous practitioners and churn out more of the same as other cybersecurity programs. We argue that the risk of workforce brittleness and fragility increases with such a narrow strategy (Taleb 2014).

Another category in the curriculum is cyber depth. The depth option allows students to select more in-depth tryout courses in different areas. The applied learning category provides options for students to include different learning modalities in their degree program. For traditional students, an internship is the recommended option.

The graduate CORe (gCORe) degree, see Table II, was designed for those interested in upskilling or pivoting. For those interested in pivoting, we have many self-paced courses to quickly build a cybersecurity foundation from fundamentals all the way to cybersecurity, Python programming, computer peripherals, and networking. These fundamentals will help students be successful in the graduate courses. Advisors work closely with students to tailor their path. Some courses will be preferred over others depending on the preferred pathway, or on course sequencing.

For those students interested in upskilling, and expanding skill sets and knowledge, the whole gCORe is available. Students can select any courses to build a degree of their choice. Some paths may be more technical while others may concentrate on governance, policy, and compliance. There are numerous options available to satisfy most pathways and interests and empower unique approaches to ultimately build a diverse workforce and foster a whole of nation effort to cyber workforce development (Whitehouse 2023).

gCORe is a workforce-based degree with culminating activities, where students can pick from teaching, publication, projects, or certification. We allowed students to complete two certifications if they so choose.

At the time of writing this paper, the CORe program has been operating successfully for two years. As is to be expected, there were many growing pains along the way and learning opportunities that the team experienced. However, the effort has been worthwhile with the stratospheric student success that BSU has witnessed thus far. Table III shows the enrollment and graduation trend since the Fall 2021 launch.

We have students who graduated gCORe after 12 months. The first cohort of uCORe graduates was in December 2022.

The breakdown of CORe program enrollment for the Spring 2023 semester is shown in Tables IV and V. The breakdown is distinct from other technical programs. We strive to continue this effort by improving the curriculum design. The minority student population is higher in uCORe. The female student is higher in gCORe than other technical degree pathways. It is our belief that these factors are due to the unique program design. We continuously review and investigate the enrollment breakdown to determine what adjustments may be applied to enhance the program.

TABLE III. CORE PROGRAM ENROLLMENT TRENDS

Program	**Fall 21**	**Spring 22**	**Summer 22**	**Fall 22**	**Spring 23**	**Summer 23**	**Fall 23**
Undergraduate CORe (uCORe)	56	99	95	170	203	174	244
uCORe Graduation	0	0	0	11	11	0	25
Graduate CORe (gCORe)	30	38	40	43	62	59	75
gCORe Graduation	0	0	2	2	6	5	9

TABLE IV. CORE RACE/ETHNICITY BREAKDOWN

Race/Ethnicity	uCORe Student	uCORe Percentage	gCORe Student	gCORe Percentage
American Indian/Alaskan Native	2	1.0%	0	0.0%
Asian	4	2.0%	4	6.5%
Black/African American	20	9.9%	5	8.1%
Hispanic/Latino	44	21.7%	6	9.7%
Native Hawaiian/Other Pacific Islander	1	0.5%	0	0.0%
No Race/Ethnicity Reported	8	3.9%	1	1.6%
Two or More Races	10	4.9%	1	1.6%
White	114	56.2%	45	72.6%
Total	203	100%	62	100%

TABLE V. CORE GENDER BREAKDOWN

Gender	uCORe Student	uCORe Percentage	gCORe Student	gCORe Percentage
Female	40	19.7%	20	32.3%
Male	163	80.3%	42	67.7%
Total	203	100%	62	100%

IV. STUDENT SUCCESS

This accessible cybersecurity program has made a significant impact on students' lives. The CORe program attracts students in 20+ states, students living in rural areas, and students who are active military and veterans. The bottom line is the program has enabled students from all walks of life to pivot to cybersecurity and this is made possible by the non-traditional, flexible, remote, and asynchronous nature of the program.

One student living in rural Idaho was able to join an international company as a cyber risk assessment intern. Others have been hired at national labs, power companies, consulting companies, semiconductor companies, local government, and state government.

Most students started with no IT/Cyber background, and through grit and hard work, they completed the coursework. Armed with cyber knowledge in support of other disciplines, students become conversant in cybersecurity using terms and context understood by employers. This trait is highly desired as cybersecurity professionals often fail to effectively communicate with co-workers outside of the security and IT departments. Those CORe students are now well positioned to take advantage of the work opportunities presented to them.

We are especially proud of those students who pivoted from non-IT/Cyber backgrounds and reinvented themselves to pivot into the field. Some students gave up nursing and found success as data and cybersecurity analysts. Others become governance and compliance experts. The stories are many and the impact is measurable. The transfer pathways for AAS students have worked out well for students and the CORe program. For students, they can complete up to 80 credit hours at community college at a lower cost, which leads to far less student debt.

V. STRENGTHS AND CHALLENGES

A. Industry Professionals as Instructors

Since BSU could not afford to hire cybersecurity professionals as full-time instructors, the program did the next best thing and hired them as adjunct instructors. BSU prepared the course descriptions and course learning outcomes and hired subject matter experts to assist in the development of different courses. This is possible through the E-campus to support the course development process. Instructional designers are there to assist in the design of the course content and structure. This structure functions well, but it requires a significant amount of upkeep. The program office must be in the loop to pick up any slack, as the professionals are adjuncts, requiring different kinds of

support, so that they can help the students. With the course content on learning management systems, students attend virtual office hours to ask instructors questions on course content and non-content. Generally speaking, non-content questions such as career questions, and advice are the most often discussed.

B. Financial Viability

CORe program is a self-supporting program. No university or state dollars are committed to the operation of the CORe program, which means that the program needs to manage spending wisely and maintain enough reserves to withstand enrollment fluctuations. The development grant and initial, and subsequent, enrollment success put CORe in a strong financial position. However, we continue to be mindful of enrollment to operate a healthy and sustainable program that can provide everything students need.

C. Enrollment

The funding needed to operate CORe programs comes from student fees. These fees are used for marketing, recruiting, advising, adjuncts hiring, and support bare minimum or skeleton full-time personnel. BSU continues to work with marketing and recruiting teams on student recruitment. The CORe program also works very closely with advising teams to make sure students are well supported to maintain retention rates.

D. Summary

The innovative CORe program has enjoyed early success. However, the program cannot be complacent. As competition heats up and changes emerge in the field of cybersecurity, the program must continue to innovate by adding new courses and content to grow the program while supporting foundational requirements and parameters. CORe continues to improve the courses and expand the group of instructors. In order to provide greater flexibility to students, more credits will be moved from required to cyber depth. This strategic restructuring will give students additional options and the flexibility to design and optimize a degree most aligned with their interests and skill sets and sets them up for success. Ultimately, the students' success is the institution's success. Without students and their success, the CORe program would not exist. In the case of CORe, this is quite literally the truth because CORe has become self-sustaining. Student's credit hours fund everything in the CORe program!

REFERENCES

[1] S.M. Loo, C, Sample, E. Enright, D. C. Shelton, C. Justice, and E. Taylor. "Building Capacity for Systems Thinking in Higher Education Cybersecurity Programs." *Journal of The Colloquium for Information Systems Security Education*, Volume 8, No. 1, Fall 2020 https://cisse.info/journal/index.php/cisse/article/view/122

[2] Meadows 2009 Meadows, Donella H. Thinking in Systems: a Primer. London; Sterling, VA: Earthscan, 2009.

[3] Bishop 2011 M. Bishop, M. Carvalho, R. For and L.M. Mayron. "Resilience is more than availability", In Proceedings of the 2011 New Security Paradigms Workshop, pp. 95 – 104, ACM, 2011.

[4] Cyberseek Cybersecurity Supply/Demand Heatmap. Website: https://www.cyberseek.org/widget-heatmap/heatmap.html

[5] Executive Order 13870 of May 2, 2019, America's Cybersecurity Workforce. Website: https://www.energy.gov/ceser/americas-cybersecurity-workforce-eo-13870

[6] Executive Order 13800 of May 11, 2017, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Website: https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[7] Policies and Priorities Federal Cybersecurity Workforce Strategy. Website: https://www.cio.gov/policies-and-priorities/cyber-workforce-strategy/

[8] Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Website: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

[9] Taleb 2014 N. Taleb, "Antifragile: Things That Gain from Disorder", Random House, 2014.

[10] Fact Sheet. Biden Harris Administration Announces National Cyber Workforce and Education Strategy. Website: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/